(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 158 826 B1

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
06.09.2006 Bulletin 2006/36

(51) Int Cl.:
H04Q 7/38 (2006.01)

(21) Application number: **01304581.0**

(22) Date of filing: **24.05.2001**

(54) **Method for processing location information relating to a terminal connected to a packet network via a cellular network**

Verfahren zum Verarbeiten von Positionsinformationen eines Endgerätes welches über ein zellulares Netzwerk an ein Paketdatennetzwerk angeschlossen ist

Procédé pour le traitement des données de position d'un terminal qui est connecté à un réseau de paquets via un réseau cellulaire

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR

(30) Priority: **24.05.2000 FI 20001252**

(43) Date of publication of application:
28.11.2001 Bulletin 2001/48

(73) Proprietor: **Nokia Corporation**
02150 Espoo (FI)

(72) Inventors:
- **Vanttinen, Veijo**
  02770 Espoo (FI)
- **Tang, Haitao**
  00700 Helsinki (FI)

(74) Representative: **Slingsby, Philip Roy et al**
Page White & Farrer
54 Doughty Street
London WC1N 2LS (GB)

(56) References cited:
WO-A-00/02406
WO-A-00/25545
WO-A-98/52379
WO-A-99/25093
US-A- 5 497 339

- **"ETSI TS 101 724 v7.2.1: Digital cellular telecommunications system (phase 2+);Location Services (LCS); (Functional description) - Stage 2 (GSM 03.71 version 7.2.1 Release 1998)" EUROPEAN TELECOMMUNICATION STANDARD, XX, XX, January 2000 (2000-01), pages 1-105, XP002144325**
- **KENT S; ATKINSON R: "RFC 2401 - Security Architecture for the Internet Protocol" INTERNET CITATION, November 1998 (1998-11), pages 1-66,**

EP 1 158 826 B1

Description

[0001] The invention relates in general to locating a device, which is connected to a packet data network via an access network. The invention relates particularly to transmitting location information from the access network to a location server in the packet data network.

[0002] In cellular networks, for example in Global System for Mobile communications (GSM), the cellular network keeps track of the location of a mobile station (MS) at least on cell level. It is also possible that the geographical location of a MS is determined. Information about the geographical location of a MS can be useful, for example, for certain services or in emergency situations.

[0003] There are various services available in the Internet. Many of these services would gain from receiving information, which indicates the location of the device asking for service. For example, an international business may have a service, which automatically gives information about the stores or service points near the user's current location. Currently it is not possible to locate an IP device connected to the Internet, other than using its IP address. An IP address, on the other hand, is not a reliable way to locate a device, as using Mobile IP it is possible to temporarily or more permanently change the location of a device without changing IP address.

[0004] In GSM, there are certain circuit-switched data services using which it is possible to have a data connection between, for example, a laptop having a card phone and a server in the Internet. General Packet Radio Service (GPRS), which is an addition to the GSM, is an example of a wireless packet switched network. GRPS and GSM, among other cellular networks, can be used as access networks to packet data networks. A packet data device can be connected to a mobile station, and via the mobile station and a cellular network, the packet data device can communicate with a packet data network. It is possible to locate the packet data device, for example, by locating the mobile station to which it is connected. It would be convenient to transmit location information about the packet data device to a server in the packet data network from an access network, for example from a cellular network. There are, however, problems relating to the confidentiality of location information and to the need of authenticating the parties who request location information.

[0005] Figure 1 presents a schematic diagram of a GSM network and a GPRS network as an example of an access network through which a packet data device can be connected to a packet data network 130. A mobile station (MS) 101 communicates with a base station (BTS) 112a. There may be, for example, a lap top computer or other packet data device 102, connected to the mobile station 101. It is also possible that the mobile station is capable of transmitting and processing packet data. In the GSM radio access network (RAN) 110, base stations are connected to base station controllers (BSC). In Figure 1 base stations 112a and 112b are connected to a base station controller (BSC) 113. The base station controller is responsible, for example, for allocation of radio resources and for handling handovers, where a mobile station changes the base station it communicates with. The base stations and base station controllers form the GSM RAN 110.

[0006] There are separate core networks for the GSM and the GPRS. A GSM core network 140 comprises in the fixed part of the network Mobile Service Switching centers (MSC), and one MSC 141, to which the BSC 113 is connected, is presented as an example in Figure 1. The GSM core network 140 is usually connected to a Public Switched Telephone Network (PSTN). The GPRS core network 120 comprises GPRS supporting nodes (GSN). Of these nodes, the one which interfaces a packet data network 130, for example the Internet, is called Gateway GPRS supporting node (GGSN). In Figure 1, a GGSN 122 is presented. Data packets may run through many GSNs, which act as routers. A mobile station or a packet data device connected to the mobile station, which is the endpoint of the data connection, is reachable through one base station controller and the GSN connected to this base station controller is called Serving GPRS support node (SGSN). In Figure 1, the mobile station 101 or device 102 is reachable via the BSC 113 and the GSN connected to this BSC is SGSN 121.

[0007] There are also network elements, which are common for the GSM and GPRS networks. In Figure 1 the common part of the GSM and GPRS networks is presented as a separate network cloud 150. The common part of the GSM and GPRS comprises, for example, Home Location Register (HLR) 151 and Visitor Location Register (VLR) 152, which take part in subscriber and mobility management. Furthermore, there is an entity called Mobile Location Center (MLC) 153, which is responsible for determining the location of a mobile station.

[0008] An entity, which is external to the GSM network, may query the location of a certain mobile station by sending a location request to a Gateway Mobile Location Center (GMLC). Figure 2 presents an example of the message sequence related to the locating of the mobile station. In Figure 2, the network elements relating to the procedure are marked with vertical lines, and the name of the entity is above each line. The messages are marked with arrows. The messages and names of the messages are given as examples; the location procedure may alternatively be carried out in a different manner than presented in Figure 2. An entity requesting the location of a certain mobile station is usually called a Location Service (LCS) Client. This entity sends a LCS request 201 to the GMLC. The LCS request comprises an identifier, for example IMSI (International Mobile Subscriber Identifier) or MSISDN, specifying the mobile station, whose location is queried. The GMLC authenticates the LCS Client to make sure that it is entitled to receive location information. After successful authentication the GMLC asks with the Routing Data message 202 the HLR, which is related to the mobile

station, the current or latest MSC, through which the mobile has been reachable; this MSC is called the Visiting MSC (VMSC). After receiving information about the VMSC from the HLR, the GMLC send a Subscriber Request 203 to this VMSC. The VMSC typically pages 204 the MS in question to receive information about the cell, in which the mobile station currently is. Thereafter the mobile station is notified of the location query with a LCS notification 205. The mobile station may either allow or refuse its location to be told. If the mobile station allows its location to be told, the VMSC asks a Serving Mobile Location Center (SMLC), which handles the location of mobile stations in the network the mobile station currently is in, to locate the mobile station with message 206. Thereafter the geographical location of the mobile station is determined. There are various possible ways to determine the location of a mobile station: the cellular network may calculate the location of a mobile station using only the information it has, the mobile station may provide some information for the location process, or the mobile station may perform the location itself, and inform the network about its current location. When the SMLC determines the location of a mobile station, various network elements, such as BSC, BS and MS itself, may be involved in the location process. The messages relating to determining the location are presented in Figure 2 with arrow 207. After the location has been determined, the SMLC returns the location information to the VMSC (message 208). The VMSC forwards the location information to the GMLC (message 209), which in turn sends a LCS response 210 to the LCS Client, which initiated the location query.

[0009] It is possible to give information about the location of a certain mobile station to a party, which is not a part of the cellular network. The LCS Client in Figure 2 is an example of such a party. The party requesting location information is usually authenticated, because location information generally needs to be treated in a confidential manner. Generally, there has to be a prenegotiated contract between the cellular network operator and the party requesting location information. When the contract is made, usually some secret authentication information (for example a shared key) is exchanged, and for each request, the party has to present it possesses this secret authentication information, for example by encrypting a part of the location request message with the secret key. The GMLC has its copy of the secret keys relating to the LCS Clients, for example. When an LCS Client, for example, tells it identity, the GMLC can then check using its copy of the a secret key that the LCS Client encrypted the text with the correct key. It is also possible to carry out a separate authentication procedure.

[0010] It is also possible to locate a packet data device 101, which is connected to a packet data network via an access network having location tracking capabilities. There may be, for example, a Location Server LS 131, which is connected to a packet data network 130, for example to the Internet. In the Internet, the identifier, which typically distinguishes devices from each other, is the IP address. The Location Server thus may know, for example, an IP address of a certain IP device. To be able to ask from a cellular network the location of the IP device, the Location Server must know to which mobile station the IP device is connected. The IP device may thus inform the Location Server, using for example a certain application and protocol designed for this purpose, about its IP address and about the MSISDN number of the mobile station connected to the IP device. The IP address may be a static IP address, which stays the same even when the location of the mobile device/station changes, or a dynamic IP address allocated, for example, by the GPRS network. If a dynamic IP address is used, there is of course some other identifier such as MSISDN which typically together tell to the Location Server the identity of the IP device.

[0011] There may be a vast number of Location Servers in the Internet. In principle, each of the Location Server operators should have a contract with each cellular network operator to ensure that it can locate an IP device which is connected to the Internet via a cellular network. The number of contracts a cellular network operator or a Location Server operator should thus make can be enormous. Furthermore, as a service in the Internet may have a short lifetime, it can be a tedious work to maintain a database, for example, containing IP addresses and authentication information of the Location Servers, which are authorized to receive location information from a cellular network. Furthermore, a packet data device connected to a packet network via an access network, for example a cellular network, may wish to authenticate a Location Server before information about the location of the packet data device is transmitted to the Location Server.

[0012] An object of the invention is to present a flexible and scalable method for processing location information relating to a packet data device, which is connected to a packet data network via an access network capable of determining location, and for providing said location information to a network element, which is connected to the packet data network, after authenticating the network element requesting the location information. A further object of the invention is that the packet data device is able to authenticate the network element requesting the location information.

[0013] Objects of the invention are achieved by establishing a security association towards a first network element, which is connected to an access network having location determination capabilities and to which location information requests from a packet data network are sent, from a second network element with the help a third network element, which second and third network elements are connected to the packet data network. Optionally a security association pointing from the second network element to the packet data device is also established.

[0014] ETSI TS101 724 "Digital cellular telecommunications system (Phase 2+); Location Services (LCS); (Functional description)-Stage 2" describes a telecommunications system capable of receiving location requests for mobile stations from location service clients.

[0015] There is provided according to the invention a packet data device according to claim 1, a mobile station according

to claim 7, a system according to claim 9 and a method according to claim 14.

[0016] Before location information is transmitted to the second network element, the second network is authenticated. This can be done by establishing a security association from the second network element to the first network element. In this description term security association refers to an agreed set of security services that are to be applied to the data transmitted from a first entity to a second entity; the unidirectional security association points towards the second entity. Each security association specifies at least one security service. Data origin authentication (authentication of the sending network element), data integrity and data encryption are examples of such security services. They may also include some details about security key management: if secret key cryptography is used, they may indicate a key distribution center, or if public key cryptography is used, they may indicate a certification center. A bi-directional security association indicates the security services to be applied on data sent to either direction between two network elements. The security services relating to a first direction may be different from those relating to the opposite direction.

[0017] Before the security services indicated by a security association can be used, the security association needs to be established. Especially in a packet data network, where there are no dedicated connections, the existence of a security association is important for being able to securely transmit data. In this description the term establishing a security association refers to a procedure, where the first network element and the second network element in a secure manner negotiate the details of a security association pointing to one of them. One way to obtain a security association is a separate contract, for example, between firms and thereafter configuring network elements so that security associations according to the contract are established. A more flexible and automatic way is to use a third network element, who is trusted by both the first network element and the second network element (or actually by the operators owning the first and second network elements), as an arbitrator. The third network element as an arbitrator can provide security documents to the first and second network elements, and using the information contained in these security documents, the first and second network element can check the origin of messages and thereafter negotiate and establish at least one security association pointing towards the first network element. It may be assumed that after a security association is set, the negotiated security services are applied on the data packets relating to that security association.

[0018] The use of a third network element as a key management center enables a first network element and a second network element to establish a security association without a previously negotiated contract. In a method according to the invention, a unidirectional security association pointing towards the first network element is sufficient for the first network element, for example, to authenticate the origin of the location request to be the second network element and to check that the location request has not been tampered. There may be a second unidirectional security association pointing towards the second network element, this security association specifying the authentication of origin. This way the second network element may check that a location response is sent by the first network element. Furthermore, to keep location information private, the second security association may indicate that the data is encrypted.

[0019] Usually the establishment of a security association is, however, not enough for transmitting location information. The first network element may check that the second network entity is allowed to receive location information or the mobile station may deny its location information to be sent to the second network element. Furthermore, the mobile station or a separate packet data device connected to the mobile station may want to set up a separate security association pointing from the second network element towards itself and thereafter check the origin of the location information request. After successfully authenticating the origin of the location information request, the location data may be transmitted to the second network element via the first network element, to which it is deliver by the cellular network using cellular network protocols. The location data may, alternatively or in addition, be transmitted from the packet data device directly to the second network element using packet data protocols, or - if the packet data device is an integral part of the mobile station - from the mobile station directly to the second network element using packet data protocols. It is possible that the location procedure of the cellular network is used only to inform the mobile station and the packet data device connected to the mobile station that the location of the packet data device is being requested. Thereafter the packet data device may determine its location without involving the cellular network and transmit the location information directly to the second network element.

[0020] The novel features which are considered as characteristic of the invention are set forth in particular in the appended Claims. The dependent claims describe some preferred embodiments of the invention. The invention itself, however, both as to its construction and its method of operation, together with additional objects and advantages thereof, will be best understood from the following description of specific embodiments when read in connection with the accompanying drawings.

Figure 1 illustrates schematically an access network capable of locating a terminal and a packet data network according to prior art,

Figure 2 illustrates a message sequence chart describing a location information transfer according to prior art,

Figure 3 illustrates schematically a key management center in a packet data network and some security associations

between the key management center and a Location Server and a Gateway Mobile Location Center,

Figure 4 illustrates a flowchart of a method according to a first preferred embodiment of the invention,

Figure 5 illustrates a message sequence chart relating to the security documents and security association establishment according to a second preferred embodiment of the invention,

Figure 6 illustrates a message sequence chart relating to the security documents and security association establishment according to a third preferred embodiment of the invention,

Figure 7 illustrates a flowchart of a method according to a fourth preferred embodiment of the invention,

Figure 8 illustrates a message sequence chart relating to the security documents and security association establishment according to the invention, and

Figure 9 illustrates a network element, a packet data device and a mobile station according to the invention.

[0021] Figures 1 - 2 are discussed in detail in the description relating to prior art.

[0022] In the following, the GSM and GPRS networks are used as an example of an access network, which is capable of locating a terminal communicating with the access network and though which it is possible to have a connection to a packet data network. Universal Mobile Telecommunication System is a further example of such an access network. Furthermore, an IP network is used as an example of a packet data network and an IP device is used as an example of a packet data device. The GMLC is used as an example of the first network element, a Location Server is used as an example of the second network element and a key management center is used as an example of the third network element.

[0023] The Internet Security Association described in Security Architecture for the Internet Protocol (RFC 2401) is an example of a security association. For the Internet Security Association it is specified that it can require data origin authentication or data encryption. A multiple of Internet Security Associations may have to be established, if both data origin authentication and data encryption are to be applied. A bi-directional security association can be implemented, for example, with two Internet Security Associations pointing to opposite directions. The actual data origin and data integrity service and data encryption service are provided by IPSec or Ipv6 protocol, when Internet Security Associations are used. Data origin and data integrity services are provided with an authentication header (AH) and data encryption with encryption of the security payload (ESP). The use of Internet Security Associations provides security services, which are applied on IP data packets. The Internet Security Associations are established, for example, using the ISAKMP protocol or Oakley key exchange protocol. Therefore it is not necessary for the network elements, which are endpoints of an Internet Security Association, to have additional applications or software in addition to the IPSec or Ipv6 and, for example, ISAKMP.

[0024] In a method according to the invention, it is also possible to use other security association than Internet Security Associations. A security association can be established between two higher-layer (above network layer) protocols or applications, too. It is also possible to tunnel a security association via some network elements, or to use transitive security associations. Transitive security association means that while there is a first security association from A to B and a second security association from B to C, there is a transitive security association from A to B.

[0025] Figure 3 illustrates Key Management Center KMC 132 and a Location Server LS 131 in a packet data network 130. It further presents in the GSM/GPRS network the Gateway Mobile Location Center GMLC 154, which is able to exchange packet data via the packet data network with the Location Server. A mobile station 101 is also illustrated, and an IP device 102 connected to the mobile station. Again, the IP device may be an integral part of the mobile station.

[0026] For the Location Server to receive location information, the GMLC has to be able to authenticate the origin of the location information request or, in other words, to be able to verify the identity the external client (Location Server) sending the location information request. One way to do this is to have an established security association, which specifies at least data origin authentication, pointing from the Location Server towards the GMLC. This security association is presented with the dashed arrow 301 in Figure 3.

[0027] The Key Management Center is involved in establishing the security association by producing a security document, which allows the GMLS to authenticate LS before or during the establishment of the security association 301. The KMC should thus be able to authenticate at least LS (either off-line beforehand or on-line during the location information request procedure) and be trusted at least by the GMLC, preferably by both the GMLC and the LS. In other words, the GMLC should accept, for example, public key certificates signed by the KMC or, if shared secrets are used, both the GMLC and the LS should each have a common shared key with the KMC. In the first case the KMC is usually called a certification agent and in the latter it is a key distribution center. The Kerberos system is one example of a key

distribution center. It is also possible that the KMC is actually a tree of key management centers, and GMLC deals with one leaf-KMC and LS deals with other leaf-KMC. Because the leaf-KMCs belong to a same tree, it is possible to create a security document, which allows the GMLC to authenticate the LS securely.

[0028] Figure 4 presents a flowchart describing a method according to the first preferred embodiment of the invention. In step 401 the GMLC receives a location information request message. Using the protocol headers of the data packet (s), for example, it may check if at least data origin authentication is applied on the data packet(s) in step 402. If no data origin authentication information is provided within the data packets, it can be assumed that there is no security association pointing from the sender towards the GMLC. Therefore the GMLC initiates security association establishment in step 403. It is also possible that the Location Server initiates the security association establishment before it requests location information; in that case the procedure starts in step 403. Details of the security association establishment are discussed below. This security association establishment involves step 404, where the KMC is asked to produce a security document relating to the sender, and step 406, where the GMLC receives the security document. Thereafter the security association establishment is carried out using at least some information provided in the security document. To receive a location information request secured with proper data origin authentication, the GMLC may in step 407 ask the sender to transmit the request again (or for the first time, if the procedure started from step 403).

[0029] If at least data origin authentication information is present in the data packet(s) relating to the location information request, after successfully authenticating the sender in step 408, the GMLC may check that the sender is authorized to receive location information in step 409. Thereafter the GMLC initiates the GSM/GPRS location procedure in step 410. The GSM/GPRS location procedure may be, for example, such a procedure as presented in Figure 2. Furthermore, it is possible that the GMLC wishes to transmit encrypted location information. In this case a second security association pointing from the GMLC towards the LS is also established.

[0030] The contents of the security document issued by the KMC depend on whether secret key or public key cryptography is used. If public key cryptography is used, the security document relating to an entity X may be a certificate $C(PK_X, ID_X; S_{KMC})$, where PK_X is the public key of X, ID_X is an identifier indicating X (typically its IP address) and S_{KMC} is a cryptographic signature produced by the KMC to prove the authenticity of the certificate. Because there usually is such a cryptographic signature in a public key certificate, it is not necessary to transmit the certificates using methods that provide data integrity and data origin authentication. If secret key cryptography is used, the KMC usually needs to know the identity of both entities X and Y involved in the security association establishment. The KMC may generate a key K_{X-Y} and place this into the security document together with an identifier ID_X. Thereafter it typically encrypts the security document using a secret key K_{KMC-Y}, which it shares with Y. The security document SD, which is delivered to Y and relates to X, may thus be $SD(ID_X, K_{X-Y}; K_{KMC-Y})$. At least the key K_{X-Y} in the security document SD is encrypted with the last argument K_{KMC-Y}. The KMC typically delivers the same secret key K_{X-Y} and identifier ID_Y in a second security document $SD(ID_Y, K_{X-Y}; K_{KMC-X})$. The key K_{KMC-X} is a shared secret between X and the KMC.

[0031] Figure 5 presents, as an example, a message sequence chart for carrying out the security association establishment according to a second preferred embodiment of the invention, where secret key cryptography is used. In Figure 5, the GMLC initiates the procedure by sending a security association establishment request 501 to the LS. The security association requested is a security association pointing towards the GMLC, and it is marked here with SA(GMLC). The request 501 may, for example, explicitly state the endpoint of the security association, or the receiver may infer the endpoint to be the sender of the request 501. The LS may, after receiving the request 501, indicate that is wishes to establish a second security association SA(LS) with a request 502. Typically the SA(LS) is requires the encryption of data. It is also possible that the GMLC asks also for the security association SA(LS), in which case the messages 501 and 502 can be single message. The LS asks the KMC for a security document relating to the GMLC with a security document request 503, and the KMC delivers the security document SD(GMLC) (message 504 in Figure 5). The security document SD(GMLC) may be, for example, $SD(ID_{GMLC}, K_{LS-GMLC}; K_{KMC-LS})$, as discussed above. Similarly, the GMLC asks the KMC for a security document relating to the LS with a security document request 505, and the KMC delivers the security document SD(LS) (message 506 in Figure 5). After receiving the security documents the GMLC and LS can establish the requested security association(s) (arrow 507 in Figure 5). Typically there is a separate protocol for establishing a security association, and authentication of each other is typically involved in security association establishment. When secret key cryptography is used, the knowledge of the key $K_{LS-GMLC}$ is usually tested in authentication. If the security associations are Internet Security Associations, the protocol to establish them is typically ISAKMP. Furthermore, it is also possible that an existing protocol such as Oakley key determination protocol or one of the other possible protocols for establishing security associations includes the messages 501-506 or similar messages.

[0032] The order of the messages and the names of the messages presented in Figure 5 are examples. The messages can be delivered in a different order. For example, as soon as the GMLC has received the location information request sent by the LS, the LS and GMLC know the identities of each other. They can ask the KMC to deliver the security documents before the security establishment requests are sent.

[0033] Figure 6 presents, as an example, a message sequence chart for carrying out the security association establishment according to a third preferred embodiment of the invention, where public key cryptography is used. When public

key certificates are used, the GMLC, for example, can ask the KMC to deliver a certificate $C(PK_{GMLC}, ID_{GMLC}; S_{KMC})$ and deliver this certificate to the LS in the security association request message. It is also possible that the LS fetches the certificate $C(PK_{GMLC}, ID_{GMLC}; S_{KMC})$ from the KMC. In Figure 6, the GMLC asks the KMC to deliver the certificate $C(PK_{GMLC}, ID_{GMLC}; S_{KMC})$, which is marked as SD(GMLC) in Figure 6 (message 503). The KMC delivers the certificate (message 504), and thereafter the GMLC sends a security association SA(GMLC) establishment request 601 to the LS. This request 601 comprises also the certificate. After the LS receives the request 601, it can authenticate GMLC. The authentication can be carried out using, for example, a challenge-and-response authentication, or the LS can check the validity of a cryptographic signature, which GMLC has placed to the request 601. If the authentication of only GMLC is sufficient for establishing the security association SA(GMCL), it can be established at this point (arrow 602). If a second security association SA(LS) is required, similar messages are exchanged between the LS and the KMC (messages 505 and 506) and between the LS and GMLC (security association SA(LS) request 603). Thereafter the security association SA(LS) can be established (arrow 604).

[0034] As discussed above, typically there is a separate protocol for establishing a security association. It is also possible that an existing protocol for establishing security associations includes the messages 601 and 602 or similar messages. The order of the messages and the names of the messages presented in Figure 6 are examples. The messages can be delivered in a different order. Public key certificates can typically be asked from a KMC (or, more precisely, from a Certification Agent CA) either online, during a certain procedure, or off-line, before the procedure. If the LS and GMLC already have a certificate of the other entity, they need not to ask them again from the KMC.

[0035] In a fourth preferred embodiment of the invention, the IP device, whose location is requested, wishes to authenticate the LS before location information is delivered to the LS. A flowchart of a method according to a fourth preferred embodiment is presented in Figure 7. The flowchart is a continuation to the flowchart in Figure 4, and it begins with step 410, where the location procedure of a cellular network is initiated. In step 701, the location procedure is carried out and at some point of the procedure a mobile station typically receives a notification that its location is requested. In Figure 7, this occurs in step 702. The mobile station may inform an IP device connected to the mobile station about the location request (step 703). The indication sent to the mobile station may comprise an identifier of the LS, and it is possible that the IP device and the Location Server authenticate each other, for example, using a shared secret on which they have beforehand agreed. Authentication using public keys is also possible. This is presented in step 704. After successful authentication, the IP device and the Location Server can agree on the encryption method used to protect to location information (step 705). The IP device may have some means of determining its location, for example a Global Positioning System receiver, and it may locate itself (step 706). Thereafter it may send the location information to the Location Server in step 707.

[0036] Figure 7 present also alternatives, where the IP device wishes to establish a security association pointing to itself from the Location Server (step 708). It is possible that the GMLC is involved as a third party in this security association establishment (step 709); this is discussed in more detail below. It is also possible that a second security association, which points from the IP device to the Location Server and specifies, for example, encryption of data, is established (step 710). The first security association allows the IP device to authenticate the Location Server. The second security association is typically used, when the IP device determines its own location (step 706), and it allows the IP device to transmit location information confidentially to the Location Server (step 707). It is also possible that the IP device authorizes the mobile station to grant a permission to transmit location information to the Location Server (step 711). In this case, it typically is sufficient to have only one security association pointing towards the IP device. After the authorization, the mobile station sends to the cellular network a message to permit the transmission of location information (step 712). If the location of the mobile station is not yet determined, the location procedure is completed at this time. The mobile station may be involved here, and even determine its own location and transmit the information via the cellular network to the GMLC. The location information is transmitted to the Location Server typically from the GMLC in step 713. The sequence of steps in Figure 7 is just an example of a method according to the invention, similarly as the alternatives presented in Figure 7. One further alternative, for example, is that the mobile station determines its location, and thereafter the IP device transmits the information to the Location Server.

[0037] In a method according to the invention, the Location Server and the IP device may thus additionally or optionally establish security associations between themselves, if they have a common key management center in the Internet. Once the IP device has authenticated the LS, it can notify the mobile station to communicate to the GMLC (or to another network entity in the cellular network) a permission to transmit the location information. One alternative for the IP device to authenticate the LS is to be involved in establishing a security association pointing from the IP device itself towards the LS. Properly selected security associations allow the LS and IP device to authenticate each other.

[0038] As discussed above, it is possible that the IP device or the LS wishes to establish security associations between the IP device and the LS, and in the Internet there may not be a common key management center which both the IP device and LS trust for their data origin authentication and payload encryption. The GMLC trusts the mobile station, as the mobile station is authenticated by the cellular network. The mobile station trusts the cellular network and the GMLC by default or through building security associations between the GMLC and the mobile station. The HRL of the mobile

station may act as a key management center for the MS and GMLC, if needed. The mobile station, furthermore, can perform mutual authentication with the IP device. This is a feasible way to establish security associations between the Location Server and the IP device, after the GMLC has authenticated the Location Server, using the GMLC as a key management center. The authentication of the Location Server can, for example, be a part of establishing a security association between the Location Server and the GMLC presented in Figures 5 and 6. Figure 8 presents a message sequence chart relating to establishment of the bi-directional security associations between the IP device and the LS *(cf.* steps 708-710 in Figure 7). The IP device asks from the GMLC an establishment of a security association towards the LS (message 801). Alternatively, this message can be sent by the Location Server. If the GMLC has not already authenticated the Location Server, the GMLC typically needs to establish security associations with the Location Server first. It may perform the procedure presented in Figure 5 or 6 at this point. If there already are, for example, bi-directional security associations between the Location Server and the GMLC enabling at least data origin authentication, then the GMLC may proceed to sending to the IP device a security document relating to the Location Server (message 802). The security document typically is a security document $SD(ID_{LS}, K_{LS\text{-}IPdevice}; K_{GMLC\text{-}IPdevice})$, and a similar security document $SD(ID_{IPdevice}, K_{LS\text{-}IPdevice}; K_{GMLC\text{-}LS})$, is sent to the Location Server (message 803). The security documents may alternatively be public key certificates issued by the GMLC, if the GMLC knows the public key of the Location Server and IP device. With the help of the information included in the security documents, the Location Server and IP device can establish a bi-directional security association between themselves (arrow 804). If the security associations are Internet Security Associations, it is possible that a multiple of unidirectional Internet Security Associations is established.

[0039] Especially if the IP device itself has positioning capability, for example there is a built-in GPS receiver in the IP device, it may wish to exchange information about its geographical location directly with a Location Server. In this case it is possible that after the mobile station receives a LCS notification, the IP device and the Location Server establish security associations between themselves and exchanges location information, as discussed above. This exchange of location information may occur, for example, in addition to the location information transmission from the GMLC to the Location Server. It is also possible that the mobile station denies the cellular network to transmit information to the Location Server, but the IP device, after authenticating the Location Server, transmits location information to the Location Server.

[0040] Figure 9 illustrates schematically a network element 900 of a cellular network according to one embodiment of the invention, a packet data device 950, which is attachable to a mobile station or an integral part of a mobile station, according to the invention and a mobile station 901 according to the invention. The network element 900, packet data device 950 and mobile station 901 may support any method according to the invention, preferably one of those described as preferred embodiments of the invention.

[0041] A network element 900 of a cellular network has the following means: means (910) for receiving from a packet data network a location information request relating to a certain mobile station, and means (920) for initiating a location procedure in the cellular network. Furthermore, it has means (930) for establishing security associations pointing to the network element from a network element of the packet data network, this security association establishment typically involving a Key management Center in a public packet data network. Further it has means (931) for performing security functions as specified by the security associations on data it receives from the packet data network, means (932) which are arranged to determine, if there is an existing security association pointing to the network element from a sender of a location information request, and means (933) for initiating security association establishment, which are arranged to establish a security association if there does not exist a security association, which points towards the network element from the sender of a location information request. Typically the means are realized using microprocessors and software. The means comprised in the security block are typically realized using Internet protocol, IPSec protocol and, for example, ISAKMP and Oakley.

[0042] The network element 900 may additionally have means (940) for receiving, for example, from an IP device reachable via the cellular network a request about a security association, which points to the network element from a certain network element of the packet data network. The network element may have means (932) for determining whether a requested security association exists, and means for transmitting (940) information about the requested security association to the device. The network element 900 may also additionally have means (943) for receiving a request to produce security documents relating to the device and to the sender of a location information request, and means (944) for producing a first security document relating to the device and a second security document relating to the sender of the location information request.

[0043] The network element 900 may be a network element of a GSM/GPRS network, preferably a Gateway Mobile Location Center, or a network element of a UMTS network.

[0044] A packet data device 950 is either an integral part of a mobile station or it is a separate device which can be attached to a mobile station. In the latter case it may be, for example, a laptop computer or a personal organizer. The packet data device 950 has means (960) for receiving information about a location information request and about a sender of a location information request from the mobile station and means (970) for exchanging with a network element connected to a cellular network information about a security association, which points to the network element from the

sender of the location information request.

[0045] The packet data device 950 may additionally have means (980) for establishing a second security association (presented as arrow 302 in Figure 3), which points to the device from the sender of the location information request and specifies at least data origin authentication. It may further have means for requesting a network element of the cellular network to produce security documents relating to the device and to the sender of the information request for the establishment of the second security association, as discussed in connection with Figure 7.

[0046] Furthermore, the packet data device 950 may have means (990) for transmitting to the mobile station a permission to send location information to the sender of the location information request, when there exists a security association pointing from the sender of the location information request to the GMLC, for example. Once the device has ascertained itself that the GMLC has authenticated the Location Server, it may decide to permit the transmission of location information. It is also possible that the packet data device 950 has means for locating itself, for example an in-built GPS receiver 995.

[0047] The mobile station 901 has means for receiving from a cellular network a notification about a location information request and means for responding to the cellular network with a notification response. It furthermore has means for notifying a device, which is attached to the mobile station, about the location information request.

[0048] The means for responding to the cellular network may expect the device to give a permission, and only thereafter send a positive response is sent to the cellular network. In other words, the means for responding to the cellular network are initiated by a permission sent by the device.

Claims

1. A packet data device (950) being an integral part of a mobile station (901) or being attachable to a mobile station (901), **characterized in that** the packet data device comprises:

   - means (960) for receiving information about a location information request relating to the packet data device and about a sender of the location information request (131) from the mobile station; and
   - means (970) for exchanging with a first network element (900) connected to a packet data network and a cellular network information about a first packet data protocol security association (507), which points to the first network element from the sender of the location information request.

2. A packet data device (950) according to claim 1, **characterized in that** it further comprises means (980) for establishing a second packet data protocol security association (804), which points to the packet data device (950) from the sender of the location information request (131) and specifies at least data origin authentication.

3. A packet data device according to claim 2, **characterized in that** it further comprises means (980) for requesting the first network element (900) to produce a first security document (803) relating to the packet data device, and a second security document (802) relating to the sender of the location information request for the establishment of the second packet data protocol security association (804).

4. A packet data device according to claim 1, **characterized in that** it further comprises means (990) for transmitting to the mobile station (901) a permission to send location information to the sender of the location information request (131), which means are arranged to transmit the permission when there is said first packet data protocol security association (507).

5. A packet data device according to claim 1, **characterized in that** it further comprises means for locating itself.

6. A packet data device according to claim 5, **characterized in that** it comprises a Global Positioning System receiver.

7. A mobile station (901) comprising or being attached to a packet data device (950) as claimed in claims 1 to 6, wherein said mobile station (901) comprises,
   means for receiving a notification from a first network element (900) connected to a packet data network and a cellular network about a location information request relating to the packet data device; and
   means for responding to the first network element (900) with a notification response, **characterized in that** it further comprises means for notifying said packet data device about the location information request.

8. A mobile station (901) according to claim 7, **characterized in that** the means for responding to the first network element (900) are arranged to be initiated by a permission sent by the packet data device (950).

9. A system comprising a packet data device (950) as claimed in claims 1 to 6, the system further comprising a first network element (900) connected to a packet data network and a cellular network having

- means (910) for receiving from a sender (131) in the packet data network a location information request relating to the packet data device,
- means (920) for initiating a location procedure in the cellular network relating to the packet data device,
- means (930) for establishing a first packet data protocol security association (507) pointing to the first network element (900) from said sender of the location information request,
- means (931) for performing security functions as specified by the first packet data protocol security association (507) on data it receives from the packet data network,
- means (932) which are arranged to determine, if there is an existing first packet data protocol security association (507), and
- means (933) for initiating packet data protocol security association establishment, which are arranged to establish the first packet data protocol security association (507) if the the first packet data protocol security association (507) does not exist
- means (940) for receiving from the packet data device (950) a request about the first packet data protocol security association (507),
- means (932) for determining whether the requested first packet data protocol security association (507) exists, and
- means (940) for transmitting information about the requested first packet data protocol security association (507) to the packet data device (950).

10. A system according to claim 9, **characterized in that** the first network element (900) further comprises

- means (943) for receiving a request to produce a first security document (803) relating to the packet data device (950) and a second security document (802,506) relating to the sender of a location information request (131), and
- means (944) for producing said first security document (803) and said second security document (802).

11. The system according to claim 9, **characterized in that** the first network element (900) is a network element of a GPRS network.

12. The system according to claim 11, **characterized in that** the first network element (900) is a Gateway Mobile Location Center.

13. The system according to claim 9, **characterized in that** the first network element (900) is a network element of a UMTS network.

14. A method (400) for processing location information which is related to a packet data device (950) as claimed in claims 1 to 6, the method comprising the step of:

- a first network element (900), which is connected to a packet data network and the cellular network, receiving (401) a location information request (201) relating to the packet data device from a sender of the location information request (131) in the packet data network, **characterized in that** the method further comprises the steps of:

  - requesting (404) from a second network element (132) which is connected to the packet data network, a second security document (506) relating to the sender of the location information request,
  - initiating the establishment (406) of at least a first packet data protocol security association (507), which specifies at least data origin authentication and points from the sender of the location information request to the first network element (900) and which establishment involves use of information comprised in the second security document (506, 802),
  - exchanging between the packet data device (950) and the first network element (900) information about the first packet data protocol security association (507),
  - after successful establishment of said first packet data protocol security association (507), authenticating (408) the sender of the location information request, and
  - if the sender of the location information request is authenticated successfully, initiating (410) a location procedure relating to the packet data device (950)in the cellular network.

15. A method according to claim 14, **characterized in that** the second security document (506) is a public key certificate which comprises an identifier specifying the sender of the location information request (131) and a public key of the sender of the location information request and which is cryptographically signed by the second network element (132).

16. A method according to claim 14, **characterized in that** it further comprises the step of:

- requesting from the second network element (132) a third security document (504) relating to the first network element (900).

17. A method according to claim 16, **characterized in that** the security document (506, 802) comprises a first key which is encrypted using a second key shared between the first network element (900) and the second network element (132), and further **characterized in that** the third security document (504) comprises the first key, which is encrypted using a third key shared between the sender of the location information request and the second network element.

18. A method according to claim 16, **characterized in that** it further comprises the step of:

- initiating the establishment of a third packet data protocol security association (507) pointing from the first network element (900) to the sender of the location information request (131) using at least information comprised in the third packet data protocol security document (504).

19. A method according to claim 18, **characterized in that** the first packet data protocol security association (507) is a set of Internet Security Associations pointing from the sender of the location information request to the first network element (900) and the third security association (507) is a second set of Internet Security Associations pointing from the first network element (900) to the sender of the location information request.

20. A method according to claim 18, **characterized in that** the third packet data protocol security association (507) specifies at least data encryption.

21. A method according to claim 14, **characterized in that** the first packet data protocol security association (507) is a set of Internet Security Associations pointing from the sender of the location information (131) request to the first network element (900).

22. A method according to claim 14, **characterized in that** it further comprises the steps of:

- said second network element (132), producing (404) said second security document (506),
- establishing (406) the first packet data protocol security association (507) using at least information comprised in the second security document (506), and
- after the establishment of the first data protocol security association (507), authenticating (408) the data origin of the sender of the location information request (131).

23. A method according to claim 22, **characterized in that** it further comprises the step of:

- transmitting (707, 713) location information relating to the packet data device (950) to the sender of the location information request (131).

24. A method according to claim 23, **characterized in that** the location information relating to the packet data device (950) is transmitted to the sender of the location information request (131) from the first network element (900).

25. A method according to claim 24, **characterized in that** it further comprises the steps of:

- the second network element producing a third security document (504) relating to the first network element, and
- establishing the third packet data protocol security association (507), which specifies at least data encryption and points from the first network element (900) to the sender of the location information request, using at least the information specified in the third security document (504).

26. A method according to claim 23, **characterized in that** it further comprises the step of:

- establishing (708) a second packet data protocol security association (804), which specifies at least data origin

authentication and points from the sender of the location information request to the packet data device (950).

27. A method according to claim 26, **characterized in that** it further comprises the step of:

- before transmission of location information, establishing (710) a fourth packet data protocol security association (804), which specifies at least data encryption and which points to the sender of the location information request (131) from said packet data device (950).

28. A method according to claim 23, **characterized in that** it further comprises the steps of:

- receiving (702) at a mobile station (901) comprising or being attached to the packet data device (950) a notification relating to the location procedure relating to the packet data device (950), and
- the mobile station informing (703) said packet data device about the notification.

29. A method according to claim 14, **characterized in that** the first network element (900) is a network element of a GPRS network.

30. A method according to claim 29, **characterized in that** the first network element (900) is a Gateway Mobile Location Center.

31. A method according to claim 14, **characterized in that** the first network element (900) is a network element of a UMTS network.

Patentansprüche

1. Paketdatenvorrichtung (950), die ein integraler Teil einer Mobilstation (901) ist oder anfügbar an eine Mobilstation (901) ist, **dadurch gekennzeichnet, dass** die Paketdatenvorrichtung umfasst:

- Mittel (960) zum Empfangen von Informationen über eine Ortsinformations-Anfrage in Zusammenhang mit der Paketdatenvorrichtung und über einen Sender der Ortsinformations-Anfrage (131) von der Mobilstation; und
- Mittel (970) zum Austauschen mit einem ersten Netzwerkelement (900), das mit einem Paketdatennetzwerk verbunden ist und Mobilfunknetzwerkinformationen über eine erste Paketdaten-Protokoll-Sicherheits-Verknüpfung (507), die von dem Sender der Ortsinformations-Anfrage auf das erste Netzwerkelement zeigt.

2. Paketdatenvorrichtung (950) nach Anspruch 1, **dadurch gekennzeichnet, dass** sie weiter Mittel (980) zum Aufbauen einer zweiten Paketdaten-Protokoll-Sicherheits-Verknüpfung (804) umfasst, die vom Sender der Ortsinformations-Anfrage (131) auf die Paketdatenvorrichtung (950) zeigt und mindestens eine Datenursprungs-Authentifizierung spezifiziert.

3. Paketdatenvorrichtung nach Anspruch 2, **dadurch gekennzeichnet, dass** sie weiter Mittel (980) zum Anfragen des ersten Netzwerkelements (900) umfasst, um ein erstes Sicherheitsdokument (803) in Zusammenhang mit der Paketdatenvorrichtung und ein zweites Sicherheitsdokument (802) in Zusammenhang mit dem Sender der Ortsinformations-Anfrage zu erzeugen, zum Aufbau der zweiten Paketdaten-Protokoll-Sicherheits-Verknüpfung (804).

4. Paketdatenvorrichtung nach Anspruch 1, **dadurch gekennzeichnet, dass** sie weiter Mittel (990) zum Übertragen einer Erlaubnis, die Ortinformation an den Sender der Ortsinformations-Anfrage (131) zu senden, an die Mobilstation (901) umfasst, wobei die Mittel eingerichtet sind, die Erlaubnis zu übertragen, wenn es die erste Paketdaten-Protokoll-Sicherheits-Verknüpfung (507) gibt.

5. Paketdatenvorrichtung nach Anspruch 1, **dadurch gekennzeichnet, dass** sie weiter Mittel zur Selbstlokalisation umfasst.

6. Paketdatenvorrichtung nach Anspruch 5, **dadurch gekennzeichnet, dass** sie einen Global-Positionierungs-System-Empfänger umfasst.

7. Mobilstation (901) umfassend oder angefügt an eine Paketdatenvorrichtung (950) nach Anspruch 1 bis 6, wobei die Mobilstation (901) umfasst,

- Mittel zum Empfangen einer Benachrichtigung von einem ersten Netzwerkelement (900), dass mit einem Paketdatennetzwerk und einem Mobilfunknetzwerk verbunden ist, über eine Ortsinformations-Anfrage in Zusammenhang mit der Paketdatenvorrichtung; und
- Mittel zum Antworten an das erste Netzwerkelement (900) mit einer Benachrichtigungsantwort, die **dadurch gekennzeichnet ist, dass** sie weiter Mittel zum Benachrichtigen der Paketdatenvorrichtung über die Ortsinformations-Anfrage umfasst.

8. Mobilstation (901) nach Anspruch 7, **dadurch gekennzeichnet, dass** die Mittel zum Antworten an das erste Netzwerkelement (900) eingerichtet sind, um durch eine Erlaubnis, die durch die Paketdatenvorrichtung (950) gesendet wurde, initiiert zu werden.

9. System umfassend eine Paketdatenvorrichtung (950) nach den Ansprüchen 1 bis 6, wobei das System weiter ein erstes Netzwerkelement (900), das mit einem Paketdatennetzwerk verbunden ist und ein Mobilfunknetzwerk umfasst, aufweisend

- Mittel (910) zum Empfangen einer Ortsinformations-Anfrage in Zusammenhang mit der Paketdatenvorrichtung, von einem Sender (131) in dem Paketdatennetzwerk,
- Mittel (920) zum Initiieren eines Ortungs-Ablaufs in dem Mobilfunknetzwerk in Zusammenhang mit der Paketdatenvorrichtung,
- Mittel (930) zum Aufbauen einer ersten Paketdaten-Protokoll-Sicherheits-Verknüpfung (507), die von dem Sender der Ortsinformations-Anfrage auf das erste Netzwerkelement (900) zeigt,
- Mittel (931) zum Ausführen von Sicherheitsfunktionen, wie spezifiziert durch die erste Paketdaten-Protokoll-Sicherheits-Verknüpfung (507) auf Daten, die sie von dem Paketdatennetzwerk empfängt,
- Mittel (932), die eingerichtet sind, festzustellen, ob es eine existierende erste Paketdaten-Protokoll-Sicherheits-Verknüpfung (507) gibt, und
- Mittel (933) zum Initiieren eines Aufbaus einer Paketdaten-Protokoll-Sicherheits-Verknüpfung, die eingerichtet sind, die erste Paketdaten-Protokoll-Sicherheits-Verknüpfung (507) aufzubauen, wenn die erste Paketdaten-Protokoll-Sicherheits-Verknüpfung (507) nicht existiert,
- Mittel (940) zum Empfangen eine Anfrage über die erste Paketdaten-Protokoll-Sicherheits-Verknüpfung (507) von der Paketdatenvorrichtung (950),
- Mittel (932) zum Feststellen, ob die angefragte erste Paketdaten-Protokoll-Sicherheits-Verknüpfung (507) existiert, und
- Mittel (940) zum Übertragen von Informationen über die angefragte erste Paketdaten-Protokoll-Sicherheits-Verknüpfung (507) an die Paketdatenvorrichtung (950).

10. System nach Anspruch 9, **dadurch gekennzeichnet, dass** das erste Netzwerkelement (900) weiter umfasst

- Mittel (943) zum Empfangen einer Anfrage, um ein erstes Sicherheitsdokument (803) in Zusammenhang mit der Paketdatenvorrichtung (950) und ein zweites Sicherheitsdokument (802, 506) in Zusammenhang mit dem Sender einer Ortsinformations-Anfrage (131) zu erzeugen, und
- Mittel (944) zum Erzeugen des ersten Sicherheitsdokuments (803) und des zweiten Sicherheitsdokuments (802).

11. System nach Anspruch 9, **dadurch gekennzeichnet, dass** das erste Netzwerkelement (900) ein Netzwerkelement eines GPRS-Netzwerks ist.

12. System nach Anspruch 11, **dadurch gekennzeichnet, dass** das erste Netzwerkelement (900) ein Gateway-Mobile-Location-Center ist.

13. System nach Anspruch 9, **dadurch gekennzeichnet, dass** das erste Netzwerkelement (900) ein Netzwerkelement eines UMTS-Netzwerks ist.

14. Verfahren (400) zum Ausführen von Ortsinformationen, die auf eine Paketdatenvorrichtung (950) nach Anspruch 1 bis 6 bezogen sind, wobei das Verfahren die Schritte umfasst:

- ein erstes Netzwerkelement (900), das mit einem Paketdatennetzwerk und dem Mobilfunknetzwerk verbunden ist, das eine Ortsinformations-Anfrage (201) in Zusammenhang mit der Paketdatenvorrichtung von einem Sender der Ortsinformations-Anfrage (131) in dem Paketdatennetzwerk empfängt (401), **dadurch gekennzeichnet,**

dass das Verfahren weiter die Schritte umfasst:
- Anfragen (404) eines zweiten Sicherheitsdokuments (506) in Zusammenhang mit dem Sender der Ortsinformations-Anfrage von einem zweiten Netzwerkelement (132), das mit einem Paketdatennetzwerk verbunden ist,
- Initiieren des Aufbaus (406) von mindestens einer Paketdaten-Protokoll-Sicherheits-Verknüpfung (507), die mindestens Datenursprungs-Authentifizierung spezifiziert und von dem Sender der Ortsinformations-Anfrage auf das erste Netzwerkelement (900) zeigt und deren Aufbau ein Verwenden von Informationen einbezieht, die in dem zweiten Sicherheitsdokument (506, 802) umfasst sind,
- Austauschen von Informationen über die erste Paketdaten-Protokoll-Sicherheits-Verknüpfung (507) zwischen der Paketdatenvorrichtung (950) und dem ersten Netzwerkelement (900),
- Authentifizieren (408) des Senders der Ortsinformations-Anfrage, nach einem erfolgreichen Aufbau der Paketdaten-Protokoll-Sicherheits-Verknüpfung (507), und
- Initiierung (410) eines Ortungs-Ablaufs in Zusammenhang mit der Paketdatenvorrichtung (950) in dem Mobilfunknetzwerk, wenn der Sender der Ortsinformations-Anfrage erfolgreich authentifiziert wird.

15. Verfahren nach Anspruch 14, **dadurch gekennzeichnet, dass** das zweite Sicherheitsdokument (506) ein öffentliches Schlüsselzertifikat ist, das einen Bezeichner, der den Sender der Ortsinformations-Anfrage (131) spezifiziert und einen öffentlichen Schlüssel des Senders der Ortsinformations-Anfrage umfasst und das durch das zweite Netzwerkelement (132) kryptografisch signiert ist.

16. Verfahren nach Anspruch 14, **dadurch gekennzeichnet, dass** es weiter die Schritte umfasst:

- Anfragen eines dritten Sicherheitsdokuments (504) in Zusammenhang mit dem ersten Netzwerkelement (900) von einem zweiten Netzwerkelement (132).

17. Verfahren nach Anspruch 16, **dadurch gekennzeichnet, dass** das Sicherheitsdokument (506, 802) einen ersten Schlüssel umfasst, der durch Verwendung eines zweiten Schlüssels verschlüsselt ist, der von dem ersten Netzwerkelement (900) und dem zweiten Netzwerkelement (132) gemeinsam genutzt wird, und weiter **dadurch gekennzeichnet, dass** das dritte Sicherheitsdokument (504) einen ersten Schlüssel umfasst, der durch Verwendung eines dritten Schlüssels verschlüsselt ist, der von dem Sender der Ortsinformations-Anfrage und dem zweiten Netzwerkelement gemeinsam genutzt wird.

18. Verfahren nach Anspruch 16, **dadurch gekennzeichnet, dass** es weiter die Schritte umfasst

- Initiieren des Aufbaus einer dritten Paketdaten-Protokoll-Sicherheits-Verknüpfung (507), die von dem ersten Netzwerkelement (900) auf dem Sender der Ortsinformations-Anfrage (131) zeigt unter Verwendung von mindestens Informationen, die in dem dritten Paketdaten-Protokoll-Sicherheits-Dokument (504) umfasst sind.

19. Verfahren nach Anspruch 18, **dadurch gekennzeichnet, dass** die erste Paketdaten-Protokoll-Sicherheits-Verknüpfung (507) ein Satz von Internet-Sicherheitsverknüpfungen ist, die von dem Sender der Ortsinformations-Anfrage auf das erste Netzwerkelement (900) zeigen und die dritte Sicherheitsverknüpfung ein zweiter Satz von Internet-Sicherheitsverknüpfungen ist, die von dem ersten Netzwerkelement (900) auf den Sender der Ortsinformations-Anfrage zeigen.

20. Verfahren nach Anspruch 18, **dadurch gekennzeichnet, dass** die dritte Paketdaten-Protokoll-Sicherheits-Verknüpfung (507) mindestens Datenverschlüsselung spezifiziert.

21. Verfahren nach Anspruch 14, **dadurch gekennzeichnet, dass** die erste Paketdaten-Protokoll-Sicherheits-Verknüpfung (507) ein Satz von Internet-Sicherheitsverknüpfungen ist, die von dem Sender der Ortsinformations (131)-Anfrage auf das erste Netzwerkelement (900) zeigen.

22. Verfahren nach Anspruch 14, **dadurch gekennzeichnet, dass** es weiter die Schritte umfasst

- Erzeugen (404) des zweiten Sicherheitsdokuments (506) durch das zweite Netzwerkelement (132),
- Aufbauen (406) der ersten Paketdaten-Protokoll-Sicherheits-Verknüpfung (507) unter Verwendung von mindestens Informationen, die in dem zweiten Sicherheitsdokument (506) umfasst sind, und
- Authentifizieren (408) des Datenursprungs des Senders der Ortsinformations-Anfrage (131). nach dem Aufbau der ersten Paketdaten-Protokoll-Sicherheits-Verknüpfung (507).

23. Verfahren nach Anspruch 22, **dadurch gekennzeichnet, dass** es weiter die Schritte umfasst:

- Übermittlung (707, 713) von Ortsinformationen im Zusammenhang mit der Paketdatenvorrichtung (950) an den Sender der Ortsinformations-Anfrage (131).

24. Verfahren nach Anspruch 23, **dadurch gekennzeichnet, dass** die Ortsinformationen in Zusammenhang mit der Paketdatenvorrichtung (950) an den Sender der Ortsinformations-Anfrage (131) von dem ersten Netzwerkelement (900) übermittelt werden.

25. Verfahren nach Anspruch 24, **dadurch gekennzeichnet, dass** es weiter die Schritte umfasst:

- Erzeugen eines dritten Sicherheitsdokuments (504) im Zusammenhang mit dem ersten Netzwerkelement durch das zweite Netzwerkelement, und
- Aufbauen der dritten Paketdaten-Protokoll-Sicherheits-Verknüpfung (507), die mindestens Datenverschlüsselung spezifiziert und von dem ersten Netzwerkelement (900) auf den Sender der Ortsinformations-Anfrage zeigt, unter Verwendung von mindestens Informationen, die in dem dritten Sicherheitsdokument (504) spezifiziert sind.

26. Verfahren nach Anspruch 23, **dadurch gekennzeichnet, dass** es weiter die Schritte umfasst:

- Aufbauen (708) einer zweiten Paketdaten-Protokoll-Sicherheits-Verknüpfung (804), die mindestens Datenursprungs-Authentifizierung spezifiziert und von dem Sender der Ortsinformations-Anfrage auf die erste Paketdatenvorrichtung (950) zeigt.

27. Verfahren nach Anspruch 26, **dadurch gekennzeichnet, dass** es weiter die Schritte umfasst:

- Aufbauen (710) einer vierten Paketdaten-Protokoll-Sicherheits-Verknüpfung (804), die mindestens Datenverschlüsselung spezifiziert und die auf den Sender der Ortsinformations-Anfrage (131) von der ersten Paketdatenvorrichtung (950) zeigt, vor der Übermittlung der Ortsinformationen.

28. Verfahren nach Anspruch 23, **dadurch gekennzeichnet, dass** es weiter die Schritte umfasst:

- Empfangen (702) eine Benachrichtigung in Zusammenhang mit dem Ortungs-Ablauf in Zusammenhang mit der Paketdatenvorrichtung (950) an einer Mobilstation (901), die die Paketdatenvorrichtung (950) umfasst oder daran angefügt ist, und
- Informieren (703) der Paketdatenvorrichtung über die Benachrichtigung durch die Mobilstation,

29. Verfahren nach Anspruch 14, **dadurch gekennzeichnet, dass** das erste Netzwerkelement (900) ein Netzwerkelement eines GPRS-Netzwerks ist.

30. Verfahren nach Anspruch 29, **dadurch gekennzeichnet, dass** das erste Netzwerkelement (900) ein Gateway-Mobile-Location-Center ist.

31. Verfahren nach Anspruch 14, **dadurch gekennzeichnet, dass** das erste Netzwerkelement (900) ein Netzwerkelement eines UMTS-Netzwerks ist.

Revendications

1. Dispositif de données par paquets (950) faisant partie intégrante d'une station mobile (901) ou pouvant être relié à une station mobile (901), **caractérisé en ce que** le dispositif de données par paquets comprend :

- un moyen (960) permettant de recevoir des informations relatives à une demande d'informations de localisation relative au dispositif de données par paquets et relative à un expéditeur de la demande d'informations de localisation (131), de la part de la station mobile ; et
- un moyen (970) permettant d'échanger, avec un premier élément de réseau (900) relié à un réseau de données par paquets et un réseau cellulaire, des informations relatives à une première association de sécurité de protocole de données par paquets (507), qui pointe vers le premier élément de réseau, provenant de l'expéditeur de la

demande d'informations de localisation.

2. Dispositif de données par paquets (950) selon la revendication 1, **caractérisé en ce qu'**il comprend en outre un moyen (980) permettant d'établir une seconde association de sécurité de protocole de données par paquets (804), qui pointe vers le dispositif de données par paquets (950), depuis l'expéditeur de la demande d'informations de localisation (131), et spécifie au moins une authentification d'origine des données.

3. Dispositif de données par paquets selon la revendication 2, **caractérisé en ce qu'**il comprend en outre un moyen (980) permettant de demander au premier élément de réseau (900) de produire un premier document de sécurité (803) relatif au dispositif de données par paquets, et un second document de sécurité (802) relatif à l'expéditeur de la demande d'informations de localisation, en vue de l'établissement de la seconde association de sécurité de protocole de données par paquets (804).

4. Dispositif de données par paquets selon la revendication 1, **caractérisé en ce qu'**il comprend en outre un moyen (990) permettant de transmettre à la station mobile (901) une permission d'envoyer des informations de localisation à l'expéditeur de la demande d'informations de localisation (131), ledit moyen étant agencé afin de transmettre la permission lorsqu'il existe ladite première association de sécurité de protocole de données par paquets (507).

5. Dispositif de données par paquets selon la revendication 1, **caractérisé en ce qu'**il comprend en outre un moyen permettant de se localiser lui-même.

6. Dispositif de données par paquets selon la revendication 5, **caractérisé en ce qu'**il comprend un récepteur de système de positionnement global.

7. Station mobile (901) comprenant ou étant reliée à un dispositif de données par paquets (950) selon les revendications 1 à 6, dans laquelle ladite station mobile (901) comprend
un moyen permettant de recevoir une notification de la part d'un premier élément de réseau (900) relié à un réseau de données par paquets et un réseau cellulaire, relative à une demande d'informations de localisation relative au dispositif de données par paquets ; et
un moyen permettant de répondre au premier élément de réseau (900) avec une réponse de notification, **caractérisée en ce qu'**elle comprend en outre un moyen permettant de notifier ledit dispositif de données par paquets au sujet de la demande d'informations de localisation.

8. Station mobile (901) selon la revendication 7, **caractérisée en ce que** le moyen permettant de répondre au premier élément de réseau (900) est agencé afin d'être déclenché par une permission envoyée par le dispositif de données par paquets (950).

9. Système comprenant un dispositif de données par paquets (950) selon les revendications 1 à 6, le système comprenant en outre un premier élément de réseau (900) relié à un réseau de données par paquets et un réseau cellulaire, possédant

- un moyen (910) permettant de recevoir, de la part d'un expéditeur (131) situé sur le réseau de données par paquets, une demande d'informations de localisation relatives au dispositif de données par paquets,
- un moyen (920) permettant de déclencher une procédure de localisation dans le réseau cellulaire, relative au dispositif de données par paquets,
- un moyen (930) permettant d'établir une première association de sécurité de protocole de données par paquets (507) pointant vers le premier élément de réseau (900), depuis ledit expéditeur de la demande d'informations de localisation,
- un moyen (931) permettant d'effectuer des fonctions de sécurité spécifiées par la première association de sécurité de protocole de données par paquets (507) sur les données qu'il reçoit de la part du réseau de données par paquets,
- un moyen (932) qui est agencé afin de déterminer si il existe ou non une première association de sécurité de protocole de données par paquets (507), et
- un moyen (933) permettant de déclencher l'établissement d'une association de sécurité de protocole de données par paquets, qui est agencé afin d'établir la première association de sécurité de protocole de données par paquets (507) si la première association de sécurité de protocole de données par paquets (507) n'existe pas,
- un moyen (940) permettant de recevoir, de la part du dispositif de données par paquets (950), une demande relative à la première association de sécurité de protocole de données par paquets (507),

- un moyen (932) permettant de déterminer si la première association de sécurité de protocole de données par paquets demandée (507) existe ou non, et
- un moyen (940) permettant de transmettre des informations relatives à la première association de sécurité de protocole de données par paquets demandée (507) au dispositif de données par paquets (950).

10. Système selon la revendication 9, **caractérisé en ce que** le premier élément de réseau (900) comprend en outre

- un moyen (943) permettant de recevoir une demande afin de produire un premier document de sécurité (803) relatif au dispositif de données par paquets (950), et un second document de sécurité (802, 506) relatif à l'expéditeur d'une demande d'informations de localisation (131), et
- un moyen (944) permettant de produire ledit premier document de sécurité (803) et ledit second document de sécurité (802).

11. Système selon la revendication 9, **caractérisé en ce que** le premier élément de réseau (900) est un élément de réseau d'un réseau GPRS.

12. Système selon la revendication 11, **caractérisé en ce que** le premier élément de réseau (900) est un centre de localisation mobile de passerelle.

13. Système selon la revendication 9, **caractérisé en ce que** le premier élément de réseau (900) est un élément de réseau d'un réseau UMTS.

14. Procédé (400) de traitement d'informations de localisation qui sont relatives à un dispositif de données par paquets (950) selon les revendications 1 à 6, le procédé comprenant l'étape consistant à :

- un premier élément de réseau (900), qui est relié à un réseau de données par paquets et au réseau cellulaire, recevant (401) une demande d'informations de localisation (201) relatives au dispositif de données par paquets, de la part d'un expéditeur de la demande d'informations de localisation (131) situé sur le réseau de données par paquets, **caractérisé en ce que** le procédé comprend en outre les étapes consistant à :

  - demander (404), depuis un second élément de réseau (132) qui est relié au réseau de données par paquets, un second document de sécurité (506) relatif à l'expéditeur de la demande d'informations de localisation,
  - déclencher l'établissement (406) d'au moins une première association de sécurité de protocole de données par paquets (507), qui spécifie au moins une authentification d'origine des données et qui pointe, depuis l'expéditeur de la demande d'informations de localisation, vers le premier élément de réseau (900), ledit établissement impliquant l'utilisation des informations comprises dans le second document de sécurité (506, 802),
  - échanger, entre le dispositif de données par paquets (950) et le premier élément de réseau (900), des informations relatives à la première association de sécurité de protocole de données par paquets (507),
  - après avoir établi ladite première association de sécurité de protocole de données par paquets avec succès (507), authentifier (408) l'expéditeur de la demande d'informations de localisation, et
  - si l'expéditeur de la demande d'informations de localisation est authentifié avec succès, déclencher (410) une procédure de localisation relative au dispositif de données par paquets (950) sur le réseau cellulaire.

15. Procédé selon la revendication 14, **caractérisé en ce que** le second document de sécurité (506) est un certificat de clé publique qui comprend un identifiant spécifiant l'expéditeur de la demande d'informations de localisation (131) et une clé publique de l'expéditeur de la demande d'informations de localisation, et qui est signé de manière cryptographique par le second élément de réseau (132).

16. Procédé selon la revendication 14, **caractérisé en ce qu'**il comprend en outre l'étape consistant à :

- demander, depuis le second élément de réseau (132), un troisième document de sécurité (504) relatif au premier élément de réseau (900).

17. Procédé selon la revendication 16, **caractérisé en ce que** le document de sécurité (506, 802) comprend une première clé qui est cryptée en utilisant une seconde clé partagée entre le premier élément de réseau (900) et le second élément de réseau (132), et **caractérisé en outre en ce que** le troisième document de sécurité (504)

comprend la première clé, qui est cryptée en utilisant une troisième clé partagée entre l'expéditeur de la demande d'informations de localisation et le second élément de réseau.

18. Procédé selon la revendication 16, **caractérisé en ce qu'**il comprend en outre l'étape consistant à :

- déclencher l'établissement d'une troisième association de sécurité de protocole de données par paquets (507) pointant, depuis le premier élément de réseau (900), vers l'expéditeur de la demande d'informations de localisation (131), en utilisant au moins les informations comprises dans le troisième document de sécurité de protocole de données par paquets (504).

19. Procédé selon la revendication 18, **caractérisé en ce que** la première association de sécurité de protocole de données par paquets (507) est un ensemble d'associations de sécurité Internet pointant, depuis l'expéditeur de la demande d'informations de localisation, vers le premier élément de réseau (900), et la troisième association de sécurité (507) est un second ensemble d'associations de sécurité Internet pointant, depuis le premier élément de réseau (900), vers l'expéditeur de la demande d'informations de localisation.

20. Procédé selon la revendication 18, **caractérisé en ce que** la troisième association de sécurité de protocole de données par paquets (507) spécifie au moins un cryptage de données.

21. Procédé selon la revendication 14, **caractérisé en ce que** la première association de sécurité de protocole de données par paquets (507) est un ensemble d'associations de sécurité Internet pointant, depuis l'expéditeur de la demande d'informations de localisation (131), vers le premier élément de réseau (900).

22. Procédé selon la revendication 14, **caractérisé en ce qu'**il comprend en outre les étapes consistant à :

- ledit second élément de réseau (132) produisant (404) ledit second document de sécurité (506),
- établir (406) la première association de sécurité de protocole de données par paquets (507) en utilisant au moins les informations comprises dans le second document de sécurité (506), et
- après l'établissement de la première association de sécurité de protocole de données par paquets (507), authentifier (408) l'origine des données de l'expéditeur de la demande d'informations de localisation (131).

23. Procédé selon la revendication 22, **caractérisé en ce qu'**il comprend en outre l'étape consistant à :

- transmettre (707, 713) des informations de localisation relatives au dispositif de données par paquets (950) à l'expéditeur de la demande d'informations de localisation (131).

24. Procédé selon la revendication 23, **caractérisé en ce que** les informations de localisation relatives au dispositif de données par paquets (950) sont transmises à l'expéditeur de la demande d'informations de localisation (131) depuis le premier élément de réseau (900).

25. Procédé selon la revendication 24, **caractérisé en ce qu'**il comprend en outre les étapes consistant à :

- le second élément de réseau produisant un troisième document de sécurité (504) relatif au premier élément de réseau, et
- établir la troisième association de sécurité de protocole de données par paquets (507), qui spécifie au moins un cryptage de données et pointe, depuis le premier élément de réseau (900), vers l'expéditeur de la demande d'informations de localisation, en utilisant au moins les informations spécifiées dans le troisième document de sécurité (504).

26. Procédé selon la revendication 23, **caractérisé en ce qu'**il comprend en outre l'étape consistant à :

- établir (708) une seconde association de sécurité de protocole de données par paquets (804), qui spécifie au moins une authentification d'origine des données et pointe, depuis l'expéditeur de la demande d'informations de localisation, vers le dispositif de données par paquets (950).

27. Procédé selon la revendication 26, **caractérisé en ce qu'**il comprend en outre l'étape consistant à :

- avant la transmission des informations de localisation, établir (710) une quatrième association de sécurité de

protocole de données par paquets (804), qui spécifie au moins un cryptage de données et pointe vers l'expéditeur de la demande d'informations de localisation (131), depuis ledit dispositif de données par paquets (950).

28. Procédé selon la revendication 23, **caractérisé en ce qu'**il comprend en outre les étapes consistant à :

- recevoir (702), au niveau d'une station mobile (901) comprenant ou étant reliée au dispositif de données par paquets (950), une notification relative à la procédure de localisation relative au dispositif de données par paquets (950), et
- la station mobile informant (703) ledit dispositif de données par paquets au sujet de la notification.

29. Procédé selon la revendication 14, **caractérisé en ce que** le premier élément de réseau (900) est un élément de réseau d'un réseau GPRS.

30. Procédé selon la revendication 29, **caractérisé en ce que** le premier élément de réseau (900) est un centre de localisation mobile de passerelle.

31. Procédé selon la revendication 14, **caractérisé en ce que** le premier élément de réseau (900) est un élément de réseau d'un réseau UMTS.

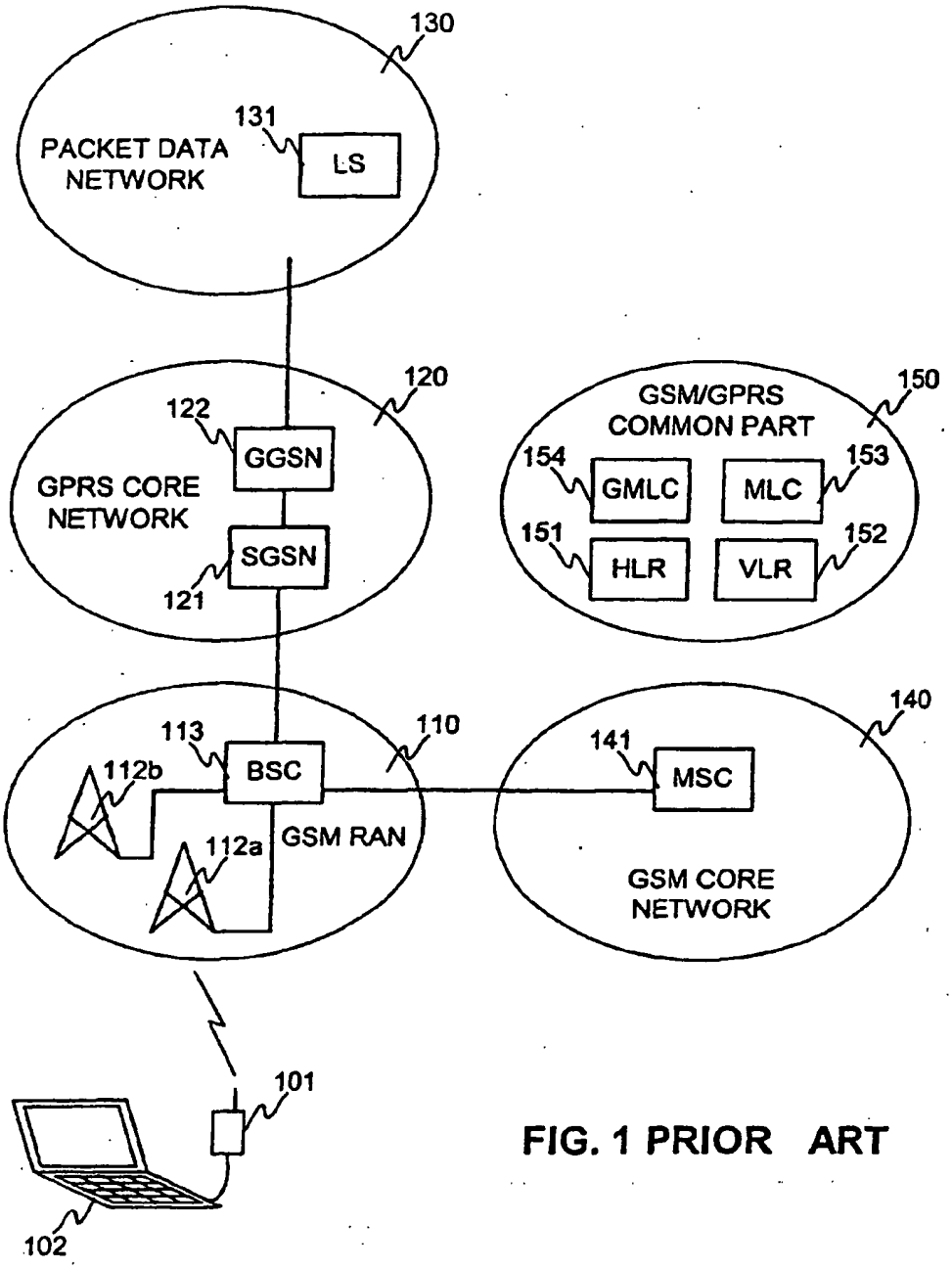

FIG. 1 PRIOR ART

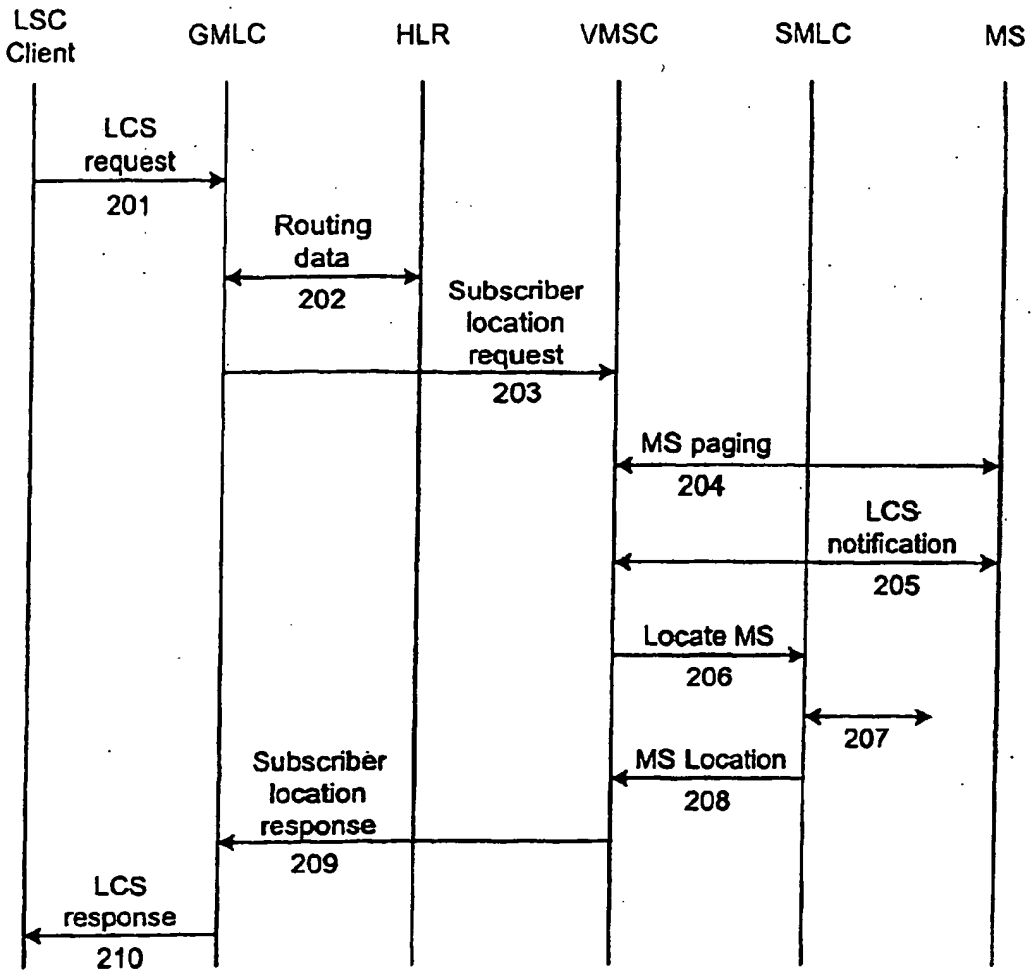

FIG. 2 PRIOR ART

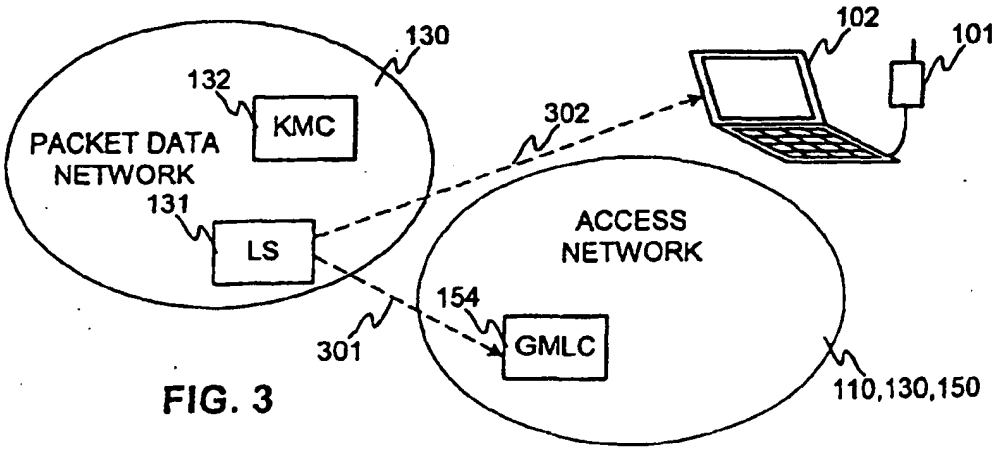

FIG. 3

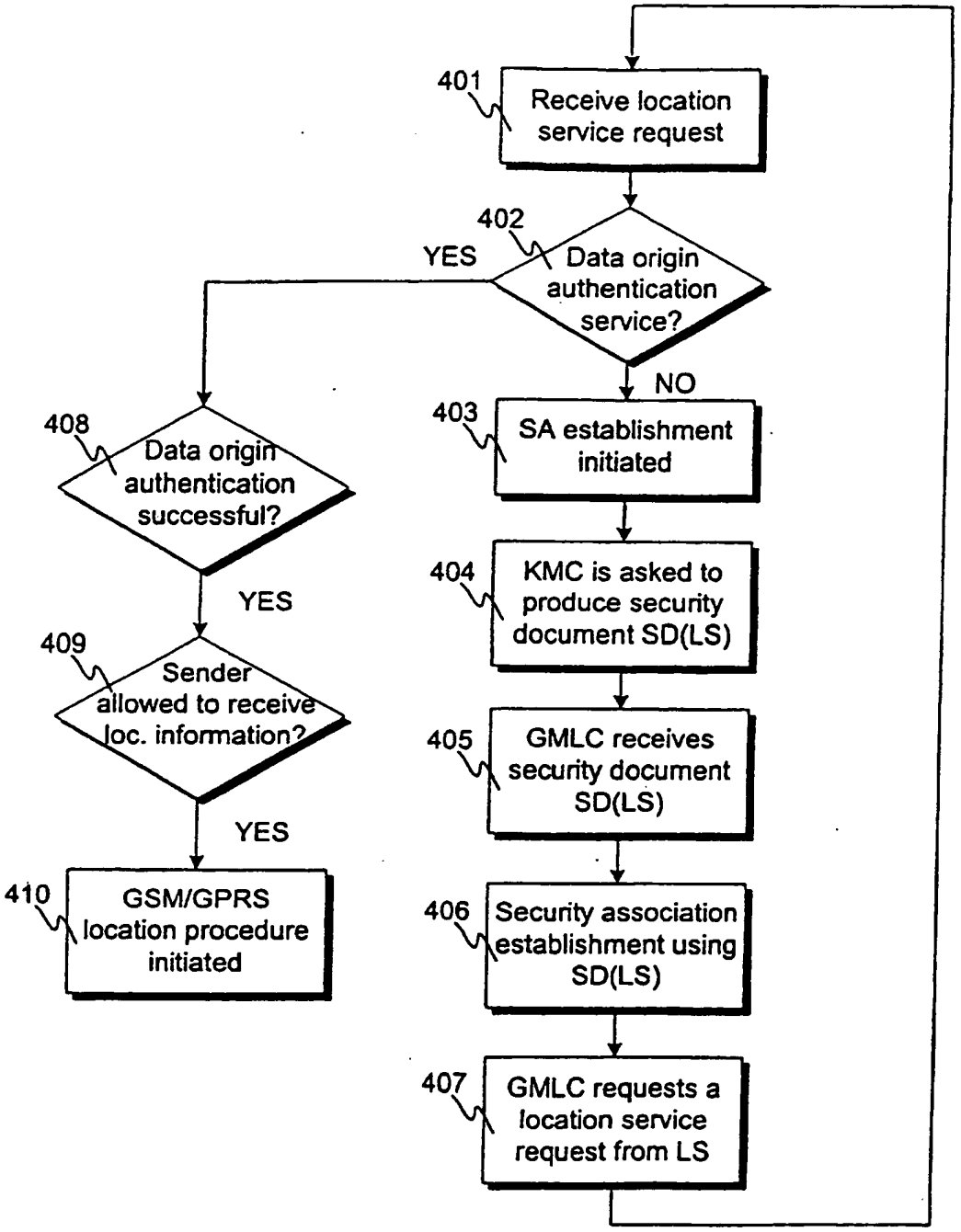
401
Receive location service request
402
Data origin authentication service?
YES
NO
403
SA establishment initiated
404
KMC is asked to produce security document SD(LS)
405
GMLC receives security document SD(LS)
406
Security association establishment using SD(LS)
407
GMLC requests a location service request from LS
408
Data origin authentication successful?
YES
409
Sender allowed to receive loc. information?
YES
410
GSM/GPRS location procedure initiated

FIG. 4

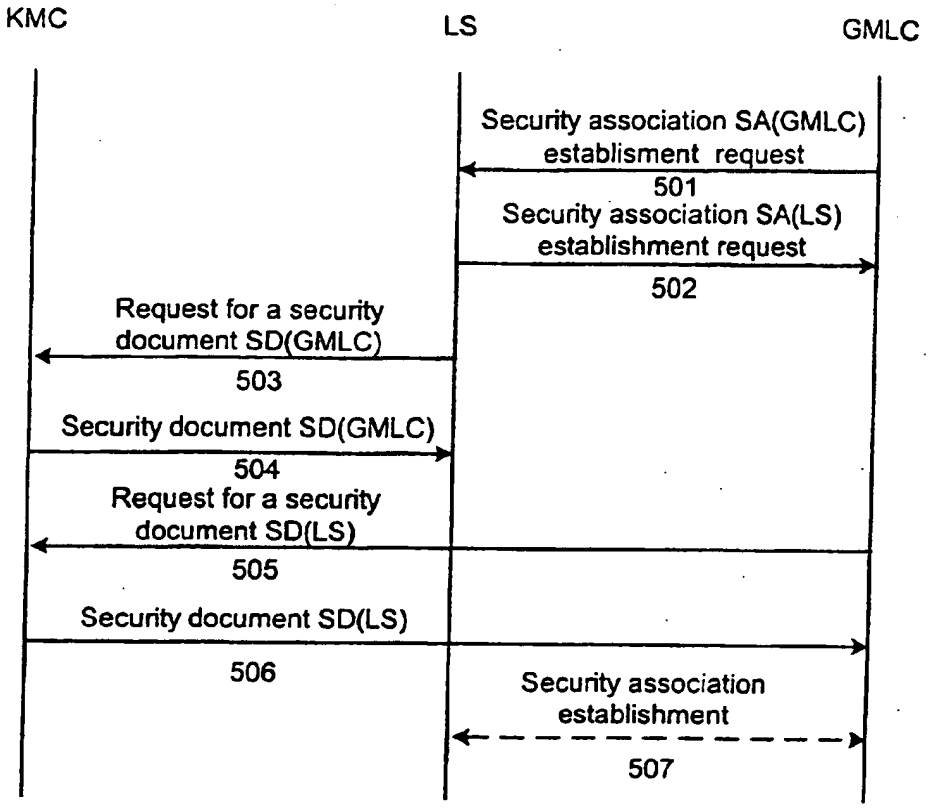
KMC
LS
GMLC
Security association SA(GMLC) establisment request
501
Security association SA(LS) establishment request
502
Request for a security document SD(GMLC)
503
Security document SD(GMLC)
504
Request for a security document SD(LS)
505
Security document SD(LS)
506
Security association establishment
507

FIG. 5

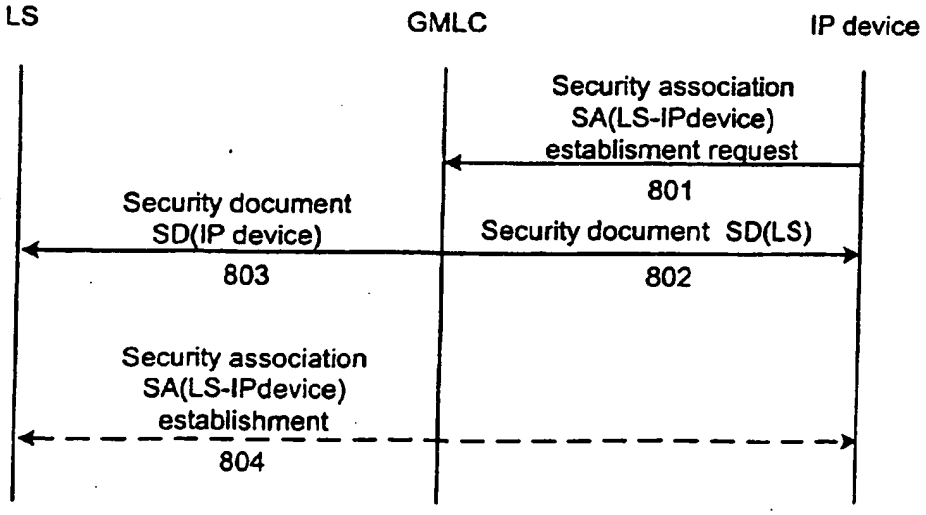
LS
GMLC
IP device
Security association SA(LS-IPdevice) establisment request
801
Security document SD(IP device)
803
Security document SD(LS)
802
Security association SA(LS-IPdevice) establishment
804

FIG. 8

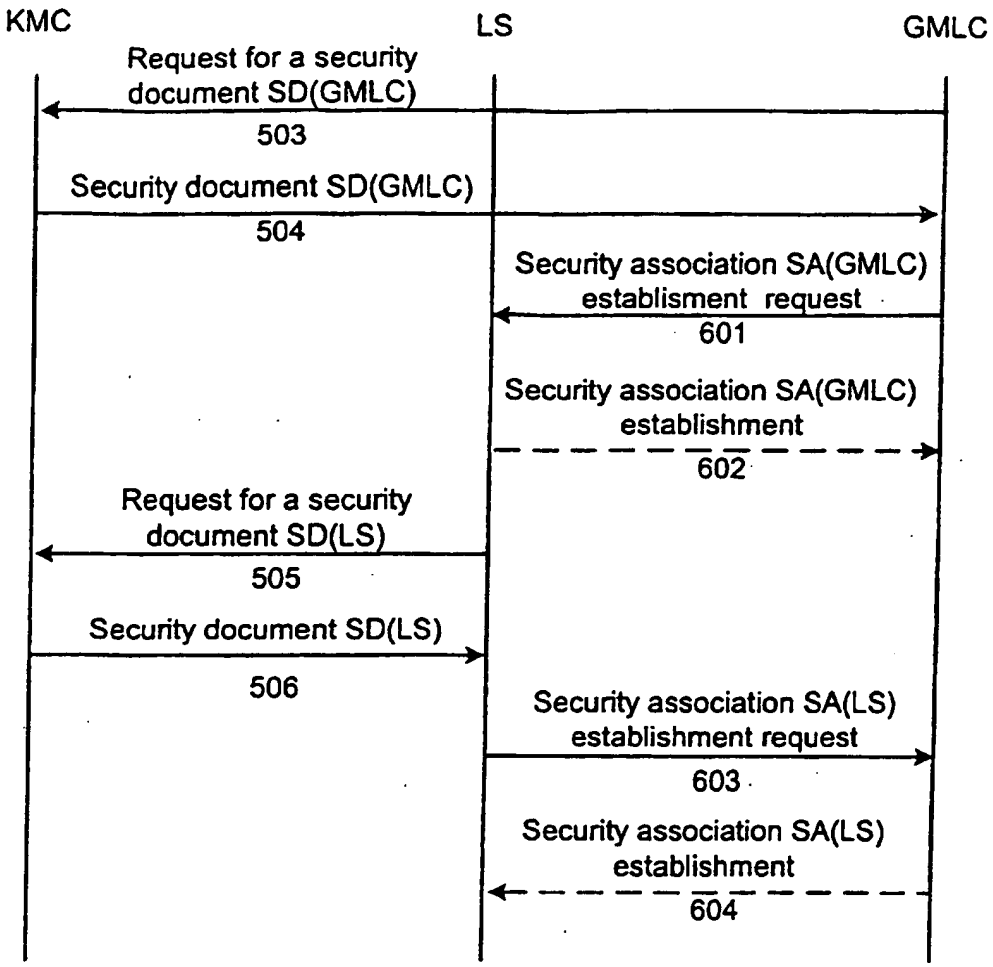
KMC
LS
GMLC
Request for a security document SD(GMLC)
503
Security document SD(GMLC)
504
Security association SA(GMLC) establisment request
601
Security association SA(GMLC) establishment
602
Request for a security document SD(LS)
505
Security document SD(LS)
506
Security association SA(LS) establishment request
603
Security association SA(LS) establishment
604

FIG. 6

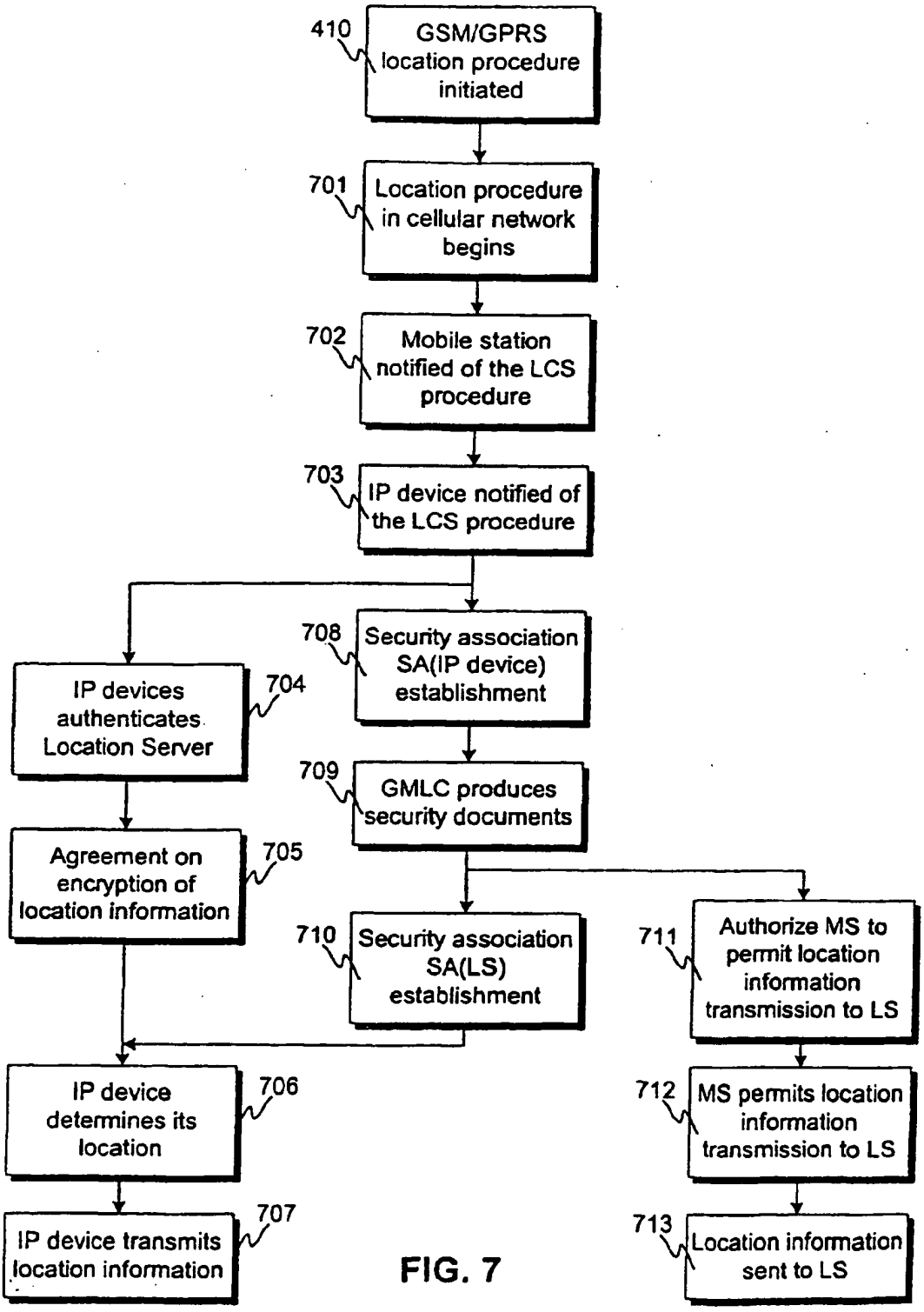
410
GSM/GPRS location procedure initiated
701
Location procedure in cellular network begins
702
Mobile station notified of the LCS procedure
703
IP device notified of the LCS procedure
708
Security association SA(IP device) establishment
704
IP devices authenticates Location Server
709
GMLC produces security documents
705
Agreement on encryption of location information
710
Security association SA(LS) establishment
711
Authorize MS to permit location information transmission to LS
706
IP device determines its location
712
MS permits location information transmission to LS
707
IP device transmits location information
713
Location information sent to LS

FIG. 7

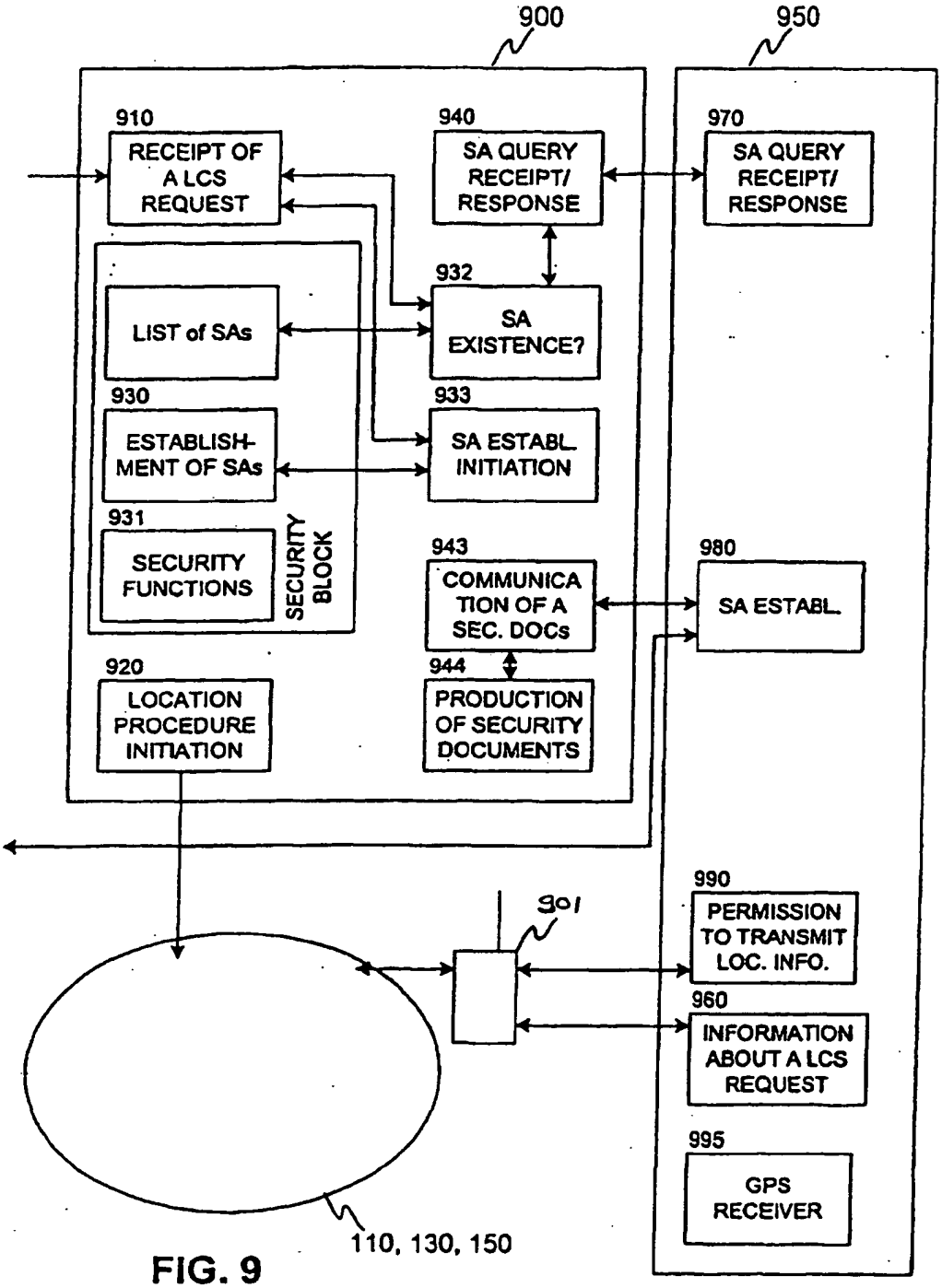
900
950
910
RECEIPT OF A LCS REQUEST
940
SA QUERY RECEIPT/ RESPONSE
970
SA QUERY RECEIPT/ RESPONSE
932
SA EXISTENCE?
LIST of SAs
930
ESTABLISH-MENT OF SAs
933
SA ESTABL. INITIATION
931
SECURITY FUNCTIONS
SECURITY BLOCK
943
COMMUNICATION OF A SEC. DOCs
980
SA ESTABL.
920
LOCATION PROCEDURE INITIATION
944
PRODUCTION OF SECURITY DOCUMENTS
901
990
PERMISSION TO TRANSMIT LOC. INFO.
960
INFORMATION ABOUT A LCS REQUEST
995
GPS RECEIVER
110, 130, 150

FIG. 9